UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/726,766	12/03/2003	Victor S. Chan	CA920030058US1	4216

58139 7590 09/24/2010

IBM CORP. (WSM)
c/o WINSTEAD SECHREST & MINICK P.C.
P.O. BOX 50784
DALLAS, TX 75201

EXAMINER	
NALVEN, ANDREW L	
ART UNIT	PAPER NUMBER
3992	

MAIL DATE	DELIVERY MODE
09/24/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte VICTOR S. CHAN, DARSHANAND KHUSIAL,
LEV MIRLAS, and WESLEY M. PHILIP

Appeal 2009-007712
Application 10/726,766
Technology Center 2400

Before JOHN A. JEFFERY, JAMES D. THOMAS, and
HOWARD B. BLANKENSHIP, *Administrative Patent Judges*.

JEFFERY, *Administrative Patent Judge*.

DECISION ON APPEAL[1]

Appellants appeal under 35 U.S.C. § 134(a) from the Examiner's rejection of claims 17-24. Claims 1-16 have been canceled. App. Br. 1. We have jurisdiction under 35 U.S.C. § 6(b). We affirm-in-part.

---

[1] The two-month time period for filing an appeal or commencing a civil action, as recited in 37 C.F.R. § 1.304, or for filing a request for rehearing, as recited in 37 C.F.R. § 41.52, begins to run from the "MAIL DATE" (paper delivery mode) or the "NOTIFICATION DATE" (electronic delivery mode) shown on the PTOL-90A cover letter attached to this decision.

STATEMENT OF THE CASE

Appellants invented a method for managing user privileges and access to electronic commerce security domains. *See generally* Spec. 3. Claim 17 is illustrative:

> 17. A method for providing user access to a portion of a web site implemented by an electronic commerce system, the web site being accessible by one or more users and comprising a set of on-line stores and a set of organizations, each of the said on-line stores being associated with one of the set of organizations, the method comprising the steps of:
>
> associating each user with a unique identity in the system;
>
> associating a user identity with one of a set of access roles for a security domain, the access role defining access privileges for the user corresponding to the user identity, the security domain comprising a subset of the set of organizations and the on-line stores associated with the organizations in the subset; and
>
> granting or denying access to a user attempting to access a portion of the web site by determining the user identity for the user and determining the access role associated with the user identity for the security domain corresponding to the portion of the web site subject to the access attempt.

The Examiner relies on the following as evidence of unpatentability:

Win	US 6,453,353 B1	Sept. 17, 2002
Gillett	US 6,760,711 B1	July 6, 2004 (filed Jan. 11, 1999)
Aull	US 7,028,180 B1	Apr. 11, 2006 (filed Oct. 16, 2000)

THE REJECTIONS

1. The Examiner rejected claims 17-23 under 35 U.S.C. § 103(a) as unpatentable over Win and Gillett. Ans. 3-5.[2,3]

2. The Examiner rejected claim 24 under 35 U.S.C. § 103(a) as unpatentable over Win, Gillett, and Aull. Ans. 5-6.

CLAIM GROUPING

Appellants argue the following claim groupings separately: (1) claims 17-19[4]; (2) claims 20-22; (3) claim 23; and (3) claim 24. *See* App. Br. 3-20; Reply Br. 2-9. Accordingly, we select claim 17 as representative of group (1). *See* 37 C.F.R. § 41.37(c)(1)(vii).

THE OBVIOUSNESS REJECTION OVER WIN AND GILLETT

Claims 17-19

Regarding representative independent claim 17, the Examiner finds that Win teaches all recited limitations, except for Win's security domain comprising a subset of the set of organizations and the on-line stores associated with the organizations in the subset. Ans. 3-4. The Examiner cites Gillett to teach this missing limitation and to provide a motivation to combine with Win. *See* Ans. 4.

---

[2] Throughout this opinion, we refer to: (1) the Appeal Brief filed March 25, 2008; (2) the Examiner's Answer mailed June 11, 2008; and (3) the Reply Brief filed August 11, 2008.

[3] The Examiner mistakenly discusses canceled claims 1-16. *See* App. Br. 1; Ans. 2-6.

[4] Claims 18 and 19 rely on the arguments made for claim 17 (*see* App. Br. 8).

Appellants argue: (1) because Gillett's server creates separate storefronts, Gillett does not teach (a) a web-site having on-line stores and organizations, and (b) a security domain consisting of a subset of organizations and on-line stores; (2) Win fails to teach granting and denying access to a web site and determining roles for a security domain; and (3) no motivation or reason has been provided to modify Win using Gillett's teachings establishing a prima facie case of obviousness. App. Br. 3-8, 12-15; Reply Br. 2-4.

The issues before us, then, are as follows:

ISSUES

(1) Under § 103, has the Examiner erred in rejecting claim 17 by finding that Win and Gillett collectively would have taught or suggested:

(a) granting or denying access to a user attempting to access a web site portion by determining the user identity;

(b) a security domain comprising a subset of organizations and on-line stores associated with the organizations in the subset; and

(c) determining the access role associated with the user identity for the security domain corresponding to the web site portion subject to the access attempt?

(2) Is the Examiner's reason to combine Win and Gillett supported by articulated reasoning with some rational underpinning to justify the Examiner's obviousness conclusion?

FINDINGS OF FACT

1. Win discloses a system 2 that enables administrators to implement access rules by defining Roles that a User plays (e.g., Employee, Customer, Supplier, Sales) when working for an organization or doing business with an enterprise. A Role may reflect a User's relationship to an organization (sales, marketing, engineering) that defines the user's information needs and access privileges. A Role also determines what resources a user can access and creates a user profile by assigning roles to a user to generate access rights. An organization registers Resources and Users of information in a central repository. Win, col. 4, ll. 44-48; col. 5, ll. 13-15, 20-32; Fig. 1.

2. Win's information sources or Resources are stored in a Web server. Win's Web resources are identified by a Uniform Resource Locator (URL), published by a Web server, and include web pages, complete web sites, and web-enabled databases. Win, col. 2, ll. 44-45; col. 5, ll. 14-21.

3. Win stores in a database: (a) information describing a user's role, a user's person type, and the functional group to which the user belongs within an enterprise; (b) a user association to the role, person type, and functional group; and (c) information describing roles and functional groups of the enterprise to which the user belongs in association with information describing the user. Based on the association, Win automatically grants access to a resource for users who have the role when the association is stored or denies access to a resource for users who do not have the role when the association is unassigned. Win, col. 2, l. 57 – col. 3, l. 6.

4. Win teaches that a user logs into the system 2 and accesses resources. If the login is successful, the system 2 presents the user with a Personalized Menu (e.g., HTML page) containing a list of authorized Resources and displays only those Resources a User can access. The custom HTML page may be based on the user's name and roles. Win, col. 5, l. 66 – col. 6, l. 16, col. 9, ll. 10-12; Fig. 1.

5. Win discusses an action carried out by Protected Server 104. A Runtime Module 206 determines whether the requested URL is a protected resource. If the resource is protected, the Module 206 calls the Authorization Verification Service to check whether a user has the right to access the resource. The process involves using a cookie sent from the user's browser to verify whether the user is authorized to access the resource. If the cookie is not verified, the user is denied access. Win, col. 6, ll. 41-65, col. 8, ll. 5-67; Figs. 1-3C.

6. Win makes web networks or web-based information accessible to external customers and suppliers to obtain information such as product catalogs and databases. Win, col. 1, ll. 45-56.

7. Gillett teaches a secure online commerce system's 20 architecture. Merchants have computer systems (e.g., 24(1)-(N)) coupled to Internet service provider (ISP) 26. The merchant computers 24(1)-(N) assisted by ISP 26 create online stores 32 hosted by the ISP 26 on behalf of merchants. An ISP's commerce server 30 helps each merchant build an online storefront (e.g., M1 Storefront, M2 Storefronts). The storefront 32 comprises a Web site with one or more web pages having products and pricing. Gillett, col. 3, l. 28 – col. 4, l. 11; col. 5, ll. 7-17; Fig. 1.

ANALYSIS

Based on the record before us, we find no error in the Examiner's obviousness rejection of representative claim 17 which calls for, in pertinent part, granting or denying access to a user attempting to access a web site portion by determining the user identity. Win discloses a system that implements access rules and defines roles that reflect a user's relationship within an organization (e.g., customer, supplier) and the user's access rights to available resources. *See* FF 1. Contrary to Appellants' assertions (App. Br. 6-8; Reply Br. 3-4), these resources include web pages and databases or a portion of a web site. *See* FF 2. Based on an association of a user to a role, a person type, and a functional group (*see* FF 3), Win determines what resources a user can access. Thus, Win teaches whether to grant or deny access to a portion of a web site based on the user. Win also customizes a user's menu (e.g., a HTML web page) based on the user's name (e.g., a user identity). *See* FF 4. Win therefore teaches granting or denying each user access to a portion of a web site by determining the user's identity (e.g., the user's name, person type, and functional group).

Win also teaches that a user can attempt to access protected resources using a cookie (e.g., yet another user identity) during an authorization process. *See* FF 5. If the user is authorized, the user is granted access to the resource. *See id.* If not, the user is denied access. *See id.* Win thus associates users and their accessible resources with the users' roles, person types, functional groups, and cookies before granting or denying a user

access to various resources. *See* FF 3-5. We therefore find that Win teaches both (1) determining the user's access role associated with a user identity, and (2) granting or denying user access to a portion of a web site by determining the user's identity as recited in claim 17.

Win further discloses that a user's role reflects a user's relationship to an organization and the organizational information (e.g., a resource) a user can access. *See* FF 1. Because a user (e.g., a customer, salesperson) will not be able to access all resources (*see* FF 1, 3-5), the access roles of a particular user relate to subset of the organizations' information or a security domain that comprises a subset of the organizations' information. Conversely, other security domains include subsets of information a user cannot access. Thus, as discussed above, when a user attempts to access one of these resources (e.g., a web page or database), Win determines the access roles associated with a user identity to decide whether a user can obtain access to the web site that is part of a security domain. *See* FF 1-5. Win therefore teaches the general concept of a security domain, as the Examiner indicates (Ans. 4).

Win also suggests making web networks and information, such as system 2, accessible to external customers and suppliers for obtaining product catalog and database information. *See* FF 6. Win, however, fails to teach explicitly that the security domain comprises a subset of organizations and on-line stores as recited in claim 17. Gillett teaches an alternative technique for organizing a security domain of an electronic commerce system. FF 7. Specifically, Gillett teaches organizations (e.g., merchants 24) and an ISP create on-line stores or web sites (e.g., M1 Storefront, M2 Storefronts) based on merchant-supplied information. *Id.*

Based on these teachings, an ordinary artisan would have recognized the benefits of including Gillett's teaching with Win. Gillett provides an architecture for building a web site that contains product and pricing information within a storefront. *See* FF 7. Contrary to Appellants' position (App. Br. 5), such an architecture for a particular storefront or web site is a subset of all the organizations and online stores. *See id.* Similarly, Win suggests that specific users (e.g., a customer, salesperson) will obtain access to a product catalog. *See* FF 1, 6. Thus, combining these teachings predictably yields no more than having a web site portion (e.g., web page or database), structured as taught by Gillett, so as to make product information and pricing available to specific user (e.g., customer, salesperson) having specific access roles. *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007). Moreover, because each user is only permitted limited access to information affiliated with user's role (*see* FF 1, 3-5), the user's identity is associated with a security domain that is a subset of the organizations and on-line stores. Thus, when the user attempts to access a portion of a website, the combined Win and Gillett system will determine the access role associated with the user's identity for the security domain corresponding to the web site portion the user has attempted to access as claim 17 requires. These teachings therefore provide a reason with some rational underpinning to justify the Examiner's conclusion of obviousness.

For the foregoing reasons, Appellants have not shown error in the rejection of claim 17 based on Win and Gillett. We therefore sustain the rejection of claim 17, and claims 18 and 19 which fall with claim 17.

Claims 20-23

Regarding claim 20, the Examiner finds that Win, as modified by Gillett, teaches the set of organizations is a tree structure. Ans. 5, 9. Specifically, the Examiner finds that Gillett teaches the tree structure's root is ISP 26, and the "leaves" or descendants of the tree structure are the merchants 24. *Id.* Appellants argue that Gillett's Figure 1 does not teach a set of organizations as a tree structure or a security domain that includes a selected organization and those organizations in the set that are descendants of the selected organization. App. Br. 8-10; Reply Br. 4-6.

The issue before us, then, is as follows:

ISSUE

(3) Under § 103, has the Examiner erred in rejecting claim 20 by finding that Win and Gillett collectively would have taught or suggested the set of organizations is a tree structure, and the security domain includes a selected organization and those organizations in the set that are descendants of the selected organization?

FINDINGS OF FACT

8. Gillett's ISP 26 includes storefronts 32 within a Commerce Server 30. The ISP 26 is connected to network 28, and network 28 is connected to merchant computers (e.g., 24(1)-(N)). Gillett, Fig. 1.

ANALYSIS

Based on the record before us, we find error in the Examiner's obviousness rejection of claim 20 which calls for, in pertinent part, the set of

organizations to be a tree structure and the security domain includes a selected organization and those organizations in the set that are descendants of the selected organization. The Examiner relies upon Gillett to teach this limitation. *See* Ans. 5, 9. While Gillett does not explicitly state that Gillett's computer architecture is a tree structure, Gillett nevertheless shows that the ISP 26 and storefronts 32 are connected to multiple merchants (e.g., 24(1)-(N)) through a network, and, in that sense, can be considered a "root" of a tree structure. *See* FF 8. But the Examiner also equates (1) Gillett's merchant computers to the recited organizations, and (2) the storefronts located in Gillett's ISP to the recited on-line stores. *See* Ans. 6-7. Thus, under this interpretation, Gillett's merchants 24 (i.e., "organizations") must form a tree structure as recited. These merchants, however, only form "leaves" of the tree structure that uses ISP 26 as its root. Also, as recited, the security domain includes a selected organization and those organizations in the set that are descendants of the selected organization. Thus, even assuming, without deciding, that Gillett's "organizations" (i.e., merchant computers) 24 could somehow be considered a "tree structure," Gillett fails to disclose the recited hierarchical arrangement, including that the security domain includes those organizations are descendants of the selected organization as claimed.

We are therefore persuaded that the Examiner erred in rejecting (1) claim 20; (2) claims 21 and 22 which recite commensurate limitations; and (3) dependent claim 23 for similar reasons. Since this issue is dispositive of our reversal of the Examiner's rejection, we need not address Appellants' other arguments (App. Br. 8-12, 15-16; Reply Br. 4-8).

THE OBVIOUSNESS REJECTION OVER WIN, GILLETT, AND AULL

Regarding claim 24, the Examiner finds that Win and Gillett teach all recited elements, except for associating[5] user identities with associated access roles occurs at the time of user registration to the web site. Ans. 5-6. The Examiner cites Aull to teach the missing limitation, and to provide a motivation to combine Aull with Win and Gillett. Ans. 6.

Appellants argue that Aull does not associate user identities with associated access roles at the time of user registration to the web site, but rather creates a role certificate. App. Br. 16-17; Reply Br. 8. Appellants also assert that Aull does not provide a sufficient reason to combine its teachings with the Win/Gillett method. App. Br. 17-20.

The issues before us, then, are as follows:

ISSUES

(4) Under § 103, has the Examiner erred in rejecting claim 24 by finding that Win, Gillett, and Aull collectively would have taught or suggested associating user identities with associated access roles occurs at the time of user registration to the web site?

(5) Is the Examiner's reason to combine Win, Gillett, and Aull supported by articulated reasoning with some rational underpinning to justify the Examiner's obviousness conclusion?

---

[5] Dependent claim 24 recites "the step of *providing* user identities with associated access roles" (emphasis added) while independent claim 17 recites "*associating* a user identity with one of a set of access roles" (emphasis added). We presume Appellants intended to recite "the step of .... associating user identities with associated access roles . . ." in claim 24.

FINDINGS OF FACT

9. Aull teaches requesting a role certificate for a user and the user's associated roles during registration with a web server. Aull, col. 9, ll. 7-21, 37-50; Fig. 2.

ANALYSIS

Based on the record before us, we find no error in the Examiner's obviousness rejection of claim 24 which calls for, in pertinent part, associating user identities with associated access roles occurs at the time of user registration to the web site. At the outset, Appellants attack Aull individually. App. Br. 16-17. However, attacking references individually does not show nonobviousness where, as here, the rejections are based on combinations of references. *In re Merck & Co., Inc.*, 800 F.2d 1091, 1097 (Fed. Cir. 1986). We therefore consider the propriety of the Examiner's rejection based on the collective teachings of Win, Gillett, and Aull.

Win's system enables user registration of the information in a central repository that contains resources identified by a URL and includes web sites. *See* FF 1-2. Win also identifies a user with specific roles based on the user's identity. *See* FF 1, 3. Win further personalizes or tailors the user's menu or web page to only the user's authorized resources that the user can access when logging into the system. FF 4. Thus, Win all but indicates that the access roles are determined when the user registers at a web site. Otherwise, such a personal menu that includes only the resources which the user has access to immediately after a successful login to the HTML page or web site (*see* FF 4) would not exist. Nonetheless, Aull confirms a known

technique of associating user with its role begins or occurs when a user commences communicating with a web server to obtain appropriate certificates for associated roles. *See* FF 9.

When considering Aull's teaching of determining and associating a user with the user's access roles at registration (*see id.*) with Win's associating user identities with associated access roles (*see* FF 1-4), this combination predictably yields no more than a skilled artisan would have expected from such an arrangement, namely associating user identities with access roles at the time a user registers with a web site. *See KSR*, 550 U.S. at 417. Moreover, accounting for an artisan's inferences and creative steps, the ordinarily skilled artisan would have recognized that determining the user's access roles upon registration would simplify and make the method more efficient by minimizing how often the method has to determine a user's access roles. *See id.* at 418; *see also Leapfrog Enter., Inc. v. Fisher-Price, Inc.*, 485 F.3d 1157, 1162 (Fed. Cir. 2007). We therefore find that Aull provides a rational underpinning for combining with Win and Gillett method.

For the foregoing reasons, Appellants have not shown error in the rejection of claim 24, and we will sustain the rejection of that claim.

CONCLUSION

Under § 103, the Examiner did not err in rejecting claims 17-19 and 24, but erred in rejecting claims 20-23.

ORDER

The Examiner's decision rejecting claims 17-24 is affirmed-in-part.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED-IN-PART

pgc

IBM CORP. (WSM)
c/o WINSTEAD SECHREST & MINICK P.C.
P.O. BOX 50784
DALLAS, TX 75201